JOHN M. CLERICI, ESQUIRE
MCKENNA LONG & ALDRIDGE LLP
WASHINGTON, D.C.

TESTIFYING ON BEHALF OF
THE CHAMBER OF COMMERCE
OF THE UNITED STATES OF AMERICA

BEFORE THE HOUSE GOVERNMENT REFORM COMMITTEE

REGARDING THE SUPPORT ANTI-TERRORISM BY FOSTERING EFFECTIVE TECHNOLOGIES ACT OF 2002 (THE "SAFETY ACT")

October 17, 2003

Mr. Chairman, Ranking Member Waxman, and Members of the Committee, it is an honor for me to testify before you today regarding the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the "SAFETY Act") and its likely impact in deploying safe and effective anti-terrorism technologies in the United States and abroad. I would like to recognize the commitment and leadership on the issue of homeland security from the Professional Services Council and the Information Technology Association of America. Finally, Mr. Chairman and Ranking Member Waxman, I applaud the leadership that both you and this Committee have shown in the areas of federal procurement policy, national security and homeland security.

I appear before you today representing the Chamber of Commerce of the United States of America. The Chamber is the world's largest business federation, representing more than three million businesses and organizations of every size, sector and region.

My testimony is based on over twenty-four months of direct experience advising large government contractors, pharmaceutical and bio-tech companies, and small businesses throughout America and throughout the world on how to bring the best possible homeland security and anti-terrorism solutions to both the government and private markets while ensuring these same companies fulfill their obligations to their owners - and in particular, their shareholders - by mitigating their risk of potential liability to the maximum extent possible. That effort culminated, in part, in the passage of the SAFETY Act in November 2002. Over the last two years, my firm has provided counsel to numerous companies selling anti-terrorism products and services, such as chemical/biological detection devices, perimeter security systems, biometric identity products, bio-defense vaccines, and airport security systems.

On July 11, 2003, the Department published in the Federal Register for notice and comment proposed implementing regulations for the SAFETY Act. On August 11, 2003, the Chamber filed comments regarding the proposed regulations. As you aware, final interim rules were published in the Federal Register just yesterday. While we are heartened that the Department has satisfactorily addressed a number of our concerns, several issues remain worthy of further comment.

Let me begin by saying that the Chamber applauds the Department of Homeland Security in its efforts to ensure that the SAFETY Act provides the full protections intended by Congress. Clearly, the interim regulations' dual goals of certainty and flexibility are in keeping with the spirit of the SAFETY Act. Most significant, the Chamber wholly endorses the Department's proper interpretation of both the jurisdictional consequences of the statute (namely, that only the Seller of designated qualified anti-terrorism technologies is a proper defendant in any action arising out of an act of terrorism when such technologies have been deployed) and

the impact of the statutory "government contract or defense" as providing early dismissal from any tort suit involving a certified qualified anti-terrorism technology following an act of terrorism.

The Chamber concurs with the Department's recognition that the "government contractor defense" referenced in the language of the SAFETY Act statutorily supplants the common law government contractor defense, thereby relieving the Seller of proving the common law elements of this defense in any tort suit filed against the Seller as a result of an act of terrorism. In such suits, the Seller would be required only to submit evidence that its qualified anti-terror technology has been "certified" by the Department under Section 863 of the Act, triggering a presumption of dismissal for the Seller and all other protections afforded by the SAFETY Act. If the SAFETY Act is to operate as Congress intends, the presumption of dismissal must not be subject to judicial permutations and interpretations of the common law government contractor defense.

We urge the Department to take appropriate actions in implementing the SAFETY Act in accordance with the interim rule to ensure that upon showing that a qualified anti-terrorism technology has been certified under Section 863 of the Act, the Seller is entitled to immediate dismissal of the action if the plaintiff fails to meet its burden to rebut this presumption.

The Chamber appreciates the Department's recognition that there exist today a number of anti-terrorism technologies that have not and cannot be deployed by Sellers unless and until they receive designation and/or certification under the SAFETY Act. The Chamber applauds this recognition and the Department's efforts to stimulate applications, including through its innovative pre-application process. The Department also acknowledges that several technologies already have been deployed without the protections of the SAFETY Act. However, while the interim rules attempt to address the issue of retroactive application of the protections of the SAFETY Act to such technologies, the Department appears to have too narrowly limited the possibility of such retroactive application. Clearly, Congress did not intend to limit the scope of the SAFETY Act to newly-developed technology.

With respect to retroactive application of the SAFETY Act, in the Chamber's view, so long as no cause of action has accrued (i.e., there has been no terrorist incident involving an anti-terror technology resulting in a lawsuit against a Seller), the Department may provide SAFETY Act protection, retroactively, to previously deployed technologies that are substantially identical to a qualified anti-terrorism technology. Nothing in the statute limits such an action. The Chamber intends to provide additional comments to urge clarification of this point in the interim rule.

With respect to the timeline for the application process itself, while the one-hundred-fifty (150) day time period provided by the interim regulations for both designation and certification under the SAFETY Act attempts to balance the need

for urgency with the requirements for certain reviews and evaluations of anti-terrorism technologies under the Act, we are concerned that this time frame is too lengthy and rigid. This is particularly true for those anti-terrorism technologies that are ready and urgently needed for deployment but which companies will not deploy until SAFETY Act coverage is provided. Early indications from the Department suggest that the application process may be unnecessarily burdensome, leading to both a lengthy review period post-application as well as extensive expenditures of Seller's resources during the application preparation process. This will, obviously, have a greater adverse impact upon small businesses where both time and money are scarce. In short, it appears the entire process - both pre and post application - may be open to further streamlining.

The interim rules note the need for the Department to retain discretion over the approval process and the Chamber, for the most part, agrees. However, the Chamber believes the decision whether to designate a technology as a qualified anti-terrorism technology and the decision whether to certify a technology as an "approved product" for purposes of the statutory government contractor defense should be subject to an internal appeal process similar to an agency-level bid protest. Under this process, the Chamber suggests that the Secretary of Homeland Security could review a decision by the Under Secretary to deny resignation and/or certification. The Chamber agrees that this decision by the Secretary should be final and not subject to further review.

Section 865(2) of the SAFETY Act defines an "act of terrorism" triggering coverage to include an act that "causes harm to a person, property, or entity, in the United States." We applaud the Department for clarifying in the interim rule that this definition does not require that the actual "act of terrorism" must occur within the boundaries of the United States, its territories or possessions. We believe that Congress intended the protections of the SAFETY Act to attach to the technology wherever deployed, so long as United States interests or citizens are harmed by an act of terrorism. Indeed, the Department itself has recognized the need to push the frontlines of protection for the homeland far beyond the natural borders of the United States by, for example, expanding U.S. Customs inspection responsibilities of sea cargo beyond domestic ports of destination to foreign ports of origin. Clearly, the providers of anti-terror technology supporting this mission are working to prevent harm to persons, property, and entities in the United States, albeit from foreign shores. Should an act of terrorism occur at a foreign port, these providers ought to enjoy the protection of the SAFETY Act.

With respect to the precise types of technologies meriting protection under the SAFETY Act, Section 865(1) of the Act notes that qualified anti-terrorism technologies may include technologies deployed for the purpose of "limiting the harm such acts [of terrorism] might otherwise cause." The "harm" that may be caused by an act of terrorism clearly goes beyond the immediate effects of the act itself. An act of terrorism such as the attacks of September 11th or the October 2001

anthrax attacks triggers a number of immediate remedial and emergency responses to limit the resulting harm and deter follow-on attacks. For example, immediately following the detection of anthrax in the offices of Senator Tom Daschle and Senator Patrick Leahy, Members of Congress and their staffs were treated with antibiotics and other prophylactic measures with the goal of limiting the harm that this act of terrorism could cause. Clearly, any injuries that might have been caused by the administration of these treatments, even though direct results of the act of terrorism itself could be directly traced to the act and the objective of limiting the resulting harm. Moreover, any claims brought as a result of such injuries would clearly be "arising out of, relating to, or resulting from an act of terrorism."

Congress recently acknowledged that technologies designed to limit the harm from an act of terrorism that may result in harm not directly caused by the act of terrorism are protected by the SAFETY Act. In the legislative history of the "Project Bioshield Act of 2002," (H.R. 2122), Congress stated that the Secretary of Homeland Security is "encouraged to designate [biodefense] countermeasures as 'qualified anti-terrorism technologies' as defined in section 862 of the Homeland Security Act." Report by Select Committee on Homeland Security to accompany H.R. 2122, July 8, 2003. Thus, the Department should affirm this Congressional statement that technologies deployed after a terrorist act with the hope of limiting resulting harm may receive designations and/or certification as qualified anti-terrorism technologies in keeping with the clear intentions of the law.

The interim rule correctly points to the intention of Congress that both the protections of the SAFETY Act and indemnification under Public Law 85-804 may, at times, be necessary for a given technology. We also note that 10 U.S.C. § 2354 provides the Department of Defense with the authority to offer indemnification for certain research and development activities. In fact, research and development institutions quite frequently engage in unusually hazardous activities related to the development of anti-terrorism technologies meriting indemnification under Public Law 85-804 and/or 10 U.S.C. § 2454.

We recommend that the Department clarify the occasions when these indemnification authorities will be used to complement the protections afforded by the SAFETY Act. For example, we suggest that Public Law 85-804 should be used on an interim basis for critical technologies that are awaiting designation and/or certification under the SAFETY Act. Otherwise, critical technologies that could protect the American people from terrorist attack or resulting harm may not be deployed solely because of liability concerns. Thus, it is important for the Department to provide further clarification on when indemnification may be appropriate in order to provide Sellers of anti-terrorism technology with the certainty the Department seeks to achieve.

We support the proposed regulations that allow the Department, in determining whether to grant the designation under Section 862, to consider

whether the proposed technology is substantially equivalent to previously designated technologies under the SAFETY Act. We urge the Department to use this concept expansively, where appropriate. For example, we suggest that the proposed regulations permit a class of services (e.g., port security) to be designated as a qualified anti-terrorism technology on the notion that substantially equivalent services that are provided at multiple locations should not be subject to multiple review processes. While the interim rule states that the Department recognizes it has the authority to grant such class designations, it appears that such class designations will not be offered immediately. We see no reason for delaying implementation of class designation as a way to streamline the process, reduce the burden on Sellers, and maximize the opportunity to bring anti-terrorism technologies to as broad a market as possible.

The Chamber appreciates that the Department has taken positive steps to more narrowly define a "substantial modification" as one that significantly reduces safety and effectiveness and its willingness to promptly review notices of modification. The interim regulations state that a "[d]esignation shall terminate automatically, and have no further force or effect, if the designated qualified anti-terrorism technology is significantly changed or modified." Given the seriousness of the loss of such designation, we strongly urge the Department to adopt a reasonable process by which it can assess whether such change has in fact occurred, with relevant input from the Seller. Unless the Department informs the Seller otherwise, the designation should remain in force, including for any changes made to the technology. Only upon a showing and a determination by the Department that there has been a significant change or modification will the Secretary be able affirmatively to terminate the designation and such termination should only take effect upon written notice to the Seller.

The interim rule requires the Secretary to establish "confidentiality protocols" with regard to the maintenance and use of information submitted to the Department by Sellers seeking designation and certification of their anti-terrorism technology under the SAFETY Act. Obviously, the information submitted to the agency will necessarily contain very sensitive confidential and proprietary commercial and technical information, including trade secrets. In addition, confidentiality is necessary to protect the information submitted from falling into the hands of potential terrorists. Moreover, such information may be sought by potential competitors to gain a competitive advantage or by the plaintiff's bar in lieu of, or as a supplement to, discovery in a tort action. Again, based upon initial indications from the Department regarding the application process, the Department appears ready to require Sellers to submit detailed financial information that goes well beyond what is required by any other government agencies. Without assurances of confidentiality, the need to supply this information alone will likely deter Sellers of qualified anti-terrorism technology from applying for SAFETY Act protections.

Finally, we are also somewhat concerned that the case law on the Freedom of Information Act ("FOIA") differentiates voluntary disclosures of information by contractors from statutorily mandated disclosures to the Federal government, and is more protective of disclosures that were not volitional. As such, applicants for designation and/or certification may be presumed to have voluntarily submitted their trade secret information and this submittal may be subject to a greater presumption toward release, even under 5 U.S.C. § 552(b)(4). Therefore, we recommend that the Department seek a specific FOIA exemption to be created for applications submitted under the SAFETY Act.

The Chamber appreciates the opportunity to offer testimony on this very important statute. Achieving the objectives of certainty and flexibility in implementing the SAFETY Act are of the utmost importance to ensuring homeland and national security. Again, we applaud your efforts, and the efforts of the Department, and look forward to full and immediate implementation of the Act.

I am happy to respond to any questions you may have.